Surveillance as a service? On the use of surveillance data for administrative purposes

Pekárek, M.E.; C Roosendaal, A.P.; Sluijs, J.P.J.B.

Published in:
European data protection

Publication date:
2013

Document Version
Peer reviewed version

Surveillance as a Service? On the Use of Surveillance Data for Administrative Purposes

Martin Pekárek[1], Arnold Roosendaal[1], and Jasper Sluijs[2]

[1] Tilburg Institute for Law, Technology, and Society (TILT), Tilburg University, The Netherlands
{m.e.pekarek,a.p.c.roosendaal}@tilburguniversity.edu
[2] Tilburg Law and Economics Center (TILEC), Tilburg University, The Netherlands
jasper.sluijs@tilburguniversity.edu

Abstract. For law enforcement purposes, authorities may either use a method of indiscriminate control or an investigative approach aimed at (finding) a particular suspect of law-breaking behavior. By applying data matching technologies, indiscriminately collected surveillance data are combined with data from other sources to select individual citizens. Inspired by insights from behavioral research, these citizens may be proactively approached in order to steer them towards desired behavior. The authorities present their communications as a service. However, selecting and addressing individual citizens tends towards investigative practices without the demonstration of any law-breaking behavior, thus straining legal certainties related to the distinction between control and investigation. Practical examples are provided through three case studies, and a number of procedural improvements are suggested to reduce the potentially intimidating character of the practices.

Keywords: surveillance, law enforcement, ANPR, behavioral research, data processing

1 Introduction

In advance of the annual tax filing due date, in 2011 the Dutch tax authority contacted a number of company car drivers. It had come to the tax authority's attention that they had registered their vehicles for professional use only, which would qualify for a tax exemption when staying under 500 'private' kilometers annually. The 500 kilometer cap may have been exceeded this year, and the agency thus kindly requested the contacted drivers to check their records to make sure their tax return would be filed correctly once due.[1]

This example comes across as a well-intentioned government policy to discourage citizens from erroneous tax filing, fitting in the proactive, service-minded and data-

[1] Sameer van Alfen, "Fiscus Bespioneert Leaserijders," *De Telegraaf*, February 11, 2011. See also Jasper Sluijs, "The Dutch Tax Authority and Lease Car Fraud: Institutionalized Intimidation," *TILT blog*, February 28, 2011, http://vortex.uvt.nl/TILTblog/?p=291.

driven ‘eGovernment’ role that many public authorities aspire to these days. However, the tax authority had reason to believe that the contacted company car drivers had in fact exceeded the 500 kilometer cap, because through Automatic Number Plate Recognition (ANPR) cameras their cars had been spotted at places that suggested extended private use of company cars — say, an IKEA parking lot on a Sunday.

When factoring into the equation how the Dutch government came to its supposition that some company car drivers may incorrectly file their taxes, this particular policy may become less benign and well-intentioned than it appears at first sight. After all, it turns out that what is presented as a service towards citizens rather seems part of a proactive measure against alleged tax fraud driven by surveillance data. The tax authority collected ANPR data and matched these data to its own administrative data on company car drivers, which yielded a number of hits on people having indicated planning to file for an exemption. The agency thus seemed to presume that the behavior of the contacted driver has been suspect, irrespective of the actual legality of their conduct.

Public authorities play a number of different roles, ranging from the execution of administrative tasks to law enforcement. In the context of law enforcement, distinct competences concerning data collection and processing tend to be strictly defined. However, the above example illustrates that authorities themselves can re-use collected data to be re-employed for administrative tasks under the moniker of a ‘service’ to citizens.

This mechanism implies that surveillance data, normally employed *ex post* as evidence against suspected offenders, is now used *ex ante* and proactively to ‘remind’ non-suspects to be law-abiding citizens. This may lead to the assumption that the service is actually an element of an encompassing surveillance and enforcement strategy. Even if this proves not to be the case, the nature and origin of the data make the service problematic because data are used in a context different from the one in which they were originally gathered. Data use in different contexts is not a new phenomenon, but in this case each context is related to a different governmental role, causing this specific type of use to raise questions in terms of foreseeability, legitimacy and accountability of government policy.

The present paper investigates and theorizes this blurring line between enforcement and administrative competences of governments, which is facilitated by data matching techniques. We attribute this recent phenomenon to the advent of behavioral research into public policy. Proactive policymaking (‘choice architecture’) more closely tailored towards actual human behavior has great advantages. The case of the Dutch tax authority nevertheless seems to suggest that pre-emptive government policy can problematize previously distinct government competences.

In this paper, we highlight a practice that can be described as the proactive use of collected surveillance data, which is enabled by recent developments in technology and data matching practices. We analyze this phenomenon, which we coin as “Surveillance as a Service”, and theorize on its underlying mechanisms and its impact on the citizens concerned. We also suggest a number of architectural and procedural measures addressing the blurring role of enforcement and administration through data matching, in which both the objectives of governments and the interests of citizens are better taken into account.

The case of the use of surveillance data to personally address citizens before any criminal offence has occurred is, to our knowledge, hitherto unique. However, it fits within the trend of proactively influencing citizen behavior towards more desirable outcomes, which is part and parcel of modern governance. To date, surveillance techniques and practices had been excluded from these practices, and the current case of the company car drivers thus represents a major crossroads in this area justifying scrutiny at the earliest opportunity. Moreover, the careful framing of the surveillance practice as a service leads to the assumption that similar procedures may be launched shortly. The analysis offered in this paper may help to instill some appropriate vigilance.

Throughout the discussion, one question may continue to linger in the background with regard to the government-initiated communication in the cases described in this paper: is it a bad thing? Or more specifically: are the rights of the citizens harmed when the authorities implement these practices? There are, *in extremo*, two possible answers to this matter. The first one is affirmative, as some observers would consider the communication unwarranted, and therefore intruding on the private life of the individuals concerned. The opposite reaction is also likely, in which people commend the proactive stance of the government, as it actively helps its citizens to prevent making mistakes. Both answers are possible, and they display two sides of the same coin, as the surveillance of citizens by the authorities always finds itself on the continuum between care and control.[2] We do not pretend to offer a moral judgment on the validity of any of these answers, which is a line of research in current surveillance studies in its own right.[3] The focus of this paper is on analyzing the novel processes at work in the presented cases. The two answers presented above only aim to underscore that some people would not conceive of the described mechanisms and associated communications strategies as being problematic at all.

The remainder of this article is structured as follows. In the next section, three specific cases are presented, each demonstrating a particular government practice subject to discussion in this paper. The section following it further develops the notion of the two faces of government, being the administrative face and the enforcement face. With regard to the latter, section 4 explores two types of enforcement (control and investigation) and highlight the differences between the two. Based on these elaborations, the case studies are addressed once again, and analyzed in terms of the government's roles and actions. After that, an alternative approach of dealing with the problems in the case studies is suggested. The paper ends with a summary and some conclusions.

2 Case studies

This section describes three case studies, which serve as a factual backdrop for the developments introduced above.

---

[2] David Lyon, *Surveillance Studies: An Overview* (Cambridge: Polity Press, 2007).

[3] See e.g., Maria Los, "Looking into the Future: Surveillance, Globalization and the Totalitarian Potential," in *Theorizing Surveillance - the panopticon and beyond*, ed. David Lyon, (Cullompton, UK: Willan Publishing, 2008), 69-94.

2.1 Private use of company cars (The Netherlands)

As part of a remuneration package, an employee can be rewarded a company car which typically may also be used for private purposes. In these cases, the benefit of using the car privately is perceived as extra income and is taxed as such. The Dutch tax code, however, states that as long as the private use of the car is lower 500 km per year, the company car is not subject to taxation.[4] To prove that the car has only be used for company purposes, the driver must keep a detailed trip registration in which every single trip is recorded, including trip purpose, starting address, destination address, the distance between the two locations as indicated by the mileage counter, etc.[5]

The driver may file a 'Statement of no private car use',[6] in which the driver states that she does not intend to use the car for private purposes for more than 500 km per year. It is important to realize that even if you have applied for a tax exemption, you are still allowed to drive your car privately as long as you stay under the 500 km cap. The trip registration must be made available to the tax authorities upon request as a control mechanism.

The issue at hand is the following. Based on ANPR data gathered during the fiscal year, the tax authorities proactively contact drivers who have expressed their intention to remain under the 500 km cap. They are reminded of the rules governing the private use of company cars, and are advised to correctly represent the facts in their communications with the tax authorities. These phone calls take place without the tax authorities having had access to the trip registration, and before there is any proof that drivers are actually committing tax fraud. The phone call is triggered by matching the list of drivers who have signed the aforementioned statement, and the vehicles present at locations that indicate private car use.[7]

2.2 Data matching to evaluate public benefits (United Kingdom)

In an effort to eliminate fraud in the public sector, the National Fraud Authority (NFA) — an executive agency of the Home Office of the United Kingdom — launched a number of pilot studies. In one of these pilots, HM Revenue & Customs (HMRC) and the Department for Work and Pensions (DWP) commissioned private-sector credit reference agencies (CRAs) and data matching companies to verify the

---

[4] Income Taxation Act 1964 (*Wet Op De Loonbelasting 1964*).

[5] The company car drivers thus have to produce surveillance data on their vehicle use, which in itself can be said to put a burden of bureaucratic precision on individual citizens.

[6] In Dutch: "Verklaring geen privégebruik auto". For a downloadable copy of the statement see: http://download.belastingdienst.nl/belastingdienst/docs/aanvraag_lh_verklaring_geen_privegebruik_auto_lh0551z3fol.pdf.

[7] The introduction of mass surveillance to verify data supplied by drivers and to then hold them accountable for behavior that is not represented in the disclosed data would only increase the burden mentioned in supra 5. It may lead to self-disciplining of citizens, an effect described in e.g. Michel Foucault, *Discipline and Punish: The Birth of the Prison* (London: Penguin Books, 1991).

circumstances of 20,000 each of benefit and tax credit claimants, in order to identify people falsely claiming to be living alone.[8]

For HMRC, CRAs identified 2,000 high-risk cases which were matched against internal HMRC data, which resulted in letters sent to 750 individuals, requesting them to either submit proof of living alone or cease to apply for this benefit claims. As a result, more than 300 claims were stopped or amended, and more savings are expected once remaining cases are followed up. For DWP, two CRAs identified between 689 and 2,598 Income Support and Jobseeker's Allowance claimants as high risk. After a match with the DWP's internal data, the department expects to save £0.5m through stopping or amending relevant benefit claims.

The relevant issue in this case is that the government's actions are taken based on information different from data originally supplied to the DWP by the citizens concerned. Instead, other data are used which have been collected and compiled by commercial entities, that do not need to adhere to the same level of accountability and transparency requirements as government institutions with regard to the source and the accuracy of data. Also, since there is no manifest proof of fraud, the government-initiated communication is presented as an administrative service, requesting the citizen to update the information on living circumstances if these, by any chance, may not represent actual arrangements anymore.

2.3 ANPR "ring of steel" (United Kingdom)

The town of Royston in Hertfordshire is allegedly the first in Britain that will have ANPR cameras on every approach to town.[9] Seven cameras around Royston will record the number plate of every vehicle that passes them, check the plate against a series of databases and send alerts to police if the vehicle is untaxed, uninsured, suspected of involvement in a crime, or appears on a local or national police "hotlist".[10] Many of the citizen's of Royston react positively or indifferently to the police initiative. However, others are more concerned. A recurring question is why so much information needs to be kept on police records if the sole objective is to catch criminals on the spot.[11]

This is one of the key elements of the complaint three civil liberties groups have filed with the information commissioner concerning the Royston initiative.[12] The organizations — No CCTV, Privacy International and Big Brother Watch — claim the project is unlawful on a number of accounts. Quoting from a 2010 report of the Hertfordshire Police Authority Scrutiny Committee, car pictures are apparently held for 90 days, and number plate pictures are held for 2 years. These retention periods

---

[8] Cabinet Office and National Fraud Authority, *Eliminating Public Sector Fraud: The Counter Fraud Taskforce Interim Report* (2011), at Annex 2.

[9] Alice Hutton, "Hidden Cameras on All Routes in," *Royston Weekly News*, March 25, 2011.

[10] Angus Batey, "Welcome to Royston … You're under Surveillance," *Guardian*, June 29, 2011.

[11] S.A. Mathieson, "Privacy Groups Take Royston's ANPR Plans to ICO," *Guardian*, June 10, 2011.

[12] Charles Farrier, Simon Davies, and Daniel Hamilton, "Complaint Letter to the Information Commissioner Concerning Royston ANPR "Ring of Steel"," June 7, 2011.

appear to be excessive when compared to similar international projects (e.g. a comparable Canadian system holds the data for only 72 hours).[13] The complaint brings a number of other issues to the fore, such as its failure to meet the requirement of necessity, which should be judged through its proportionality and subsidiarity. At least with regard to proportionality there seem to be problems with the justification of the "ring of steel". Its lawfulness is further challenged by the lack of a specified purpose, and the claimants put forward that generic objectives like "the prevention and detection of crime, public disorder, terrorism and to remove from public roads both unsafe vehicles and unsafe drivers" are far too general to justify the mass collection of data.

For the purposes of this paper, the relevant issue in this case is that enforcement agencies are collecting all license plate information as a matter of routine using blanket surveillance practices, and retain this information for up to two years without any justifying cause. Because of the lack of any specified goal for this mass collection of data, it may be put to any use in the months and years to come for aims that by definition are unknown at the time of registration. A database with two years of individualized movement data can be mined to discover all sorts of correlations that should be of no interest to a police force if there is no explicit goal whose legitimacy can be challenged in a court of law. The ANPR registration thus puts a liability on the future of everyone whose license plate has been scanned, because developments beyond the control of the individuals concerned may brand them as a potential target for unwarranted police scrutiny in the future, only because their vehicle has crossed the town's limits in the past.

3 Proactive government: a modern twist to classic roles

This section outlines the phenomenon we coin as 'surveillance as a service,' and theorizes this concept as part of the trend towards more proactive government policy-making that countries like the US, UK and the Netherlands pursue, often based on behavioral insights.

Governments in western democracies these days seem receptive towards insights from behavioral (economic) research, which has been popularized by authors like Cass Sunstein and Richard Thaler.[14] Behavioral economics departs from the idea that consumers act as non-rational actors in economic transactions, which is contrary to the basic premises of neo-classical economics.[15] This idea of non-rationality is based

[13] Information and Privacy Commissioner/Ontario, "Privacy Investigation: The Toronto Police Service's Use of Mobile Licence Plate Recognition Technology to Find Stolen Vehicles," (2003).

[14] Richard H. Thaler and Cass R. Sunstein, *Nudge: Improving Decisions About Health, Wealth, and Happiness*, 1st ed. (Yale University Press, 2008).

[15] See e.g., Christine Jolls, Cass R. Sunstein and Richard H. Thaler, "A Behavioral Approach to Law and Economics," *Stanford Law Review* 50 (1997): 1471-1550.

on experimental research demonstrating that 'real' people in a lab environment do not rationally maximize welfare as assumed by traditional economic theory.[16]

The findings of behavioral economic research have trickled down into policy circles,[17] leading to innovative ways of 'libertarian paternalistic' policymaking ranging from more efficient ways of registering organ donors via an opt-out mechanism, to incentivizing citizens towards behavior that is more friendly to the environment. Particularly the British government has been very susceptive to behavioral research,[18] where prime minister Cameron even instantiated a 'Behavioral Insights Team' (BIT) as part of the Cabinet Office, whose aim it its to help the UK government develop and apply lessons from behavioral economics and behavioral science to public policy making. In short, it supports government departments in designing policy that better reflects how people really behave, not how they are assumed to behave.[19]

Similar initiatives have been introduced informally in neighboring countries, such as the Netherlands.[20] The British BIT has sparked initiatives in fields as diverse as healthcare, consumer empowerment and energy efficiency.[21] Interestingly, the BIT also endeavors to use behavioral research to fight fraud and other forms of crime and as such collaborates with the also newly instantiated National Fraud Authority (NFA) — also a part of the Cabinet Office. The two groups jointly worked on a successful project where people who had overdue tax debt the year before were contacted informally the next year and were notified of how many people in their region had already filed their taxes on time. This prompted more of these people to file their taxes before the due date.[22]

This successful collaboration between the BIT and NFA was premised on a data matching methodology: a dataset on tax payment of individuals was combined with residential records. Indeed, data matching is a methodology often used to counter fraud, in which formerly unrelated databases are matched to detect fraudulent behavior. Data matching has been embraced enthusiastically by governments,[23] and is increasingly framed by public authorities as well as a way to make relations between citizens and governments more efficient in similar ways as behavioral research is

---

[16] For a brief outline of the methodology of behavioral economic research, see: George Loewenstein, "Experimental Economics from the Vantage-Point of Behavioural Economics," *The Economic Journal* 109, February (1999): F25-F34..

[17] Richard H. Thaler and Cass R. Sunstein, "Libertarian Paternalism," *The American Economic Review* 93 (2003): 175-179.

[18] David Wintour, "David Cameron's 'Nudge Unit' Aims to Improve Economic Behaviour," *Guardian*, September 9, 2010.

[19] Gus O'Donnell, "Applying Behavioural Insights," Cabinet Office, accessed November 29, 2011, http://www.cabinetoffice.gov.uk/content/applying-behavioural-insights.

[20] Peter Kooreman and Henriëtte Prast, "What Does Behavioral Economics Mean for Policy? Challenges to Savings and Health Policies in the Netherlands," *De Economist* 158, no. 2 (2010): 101-122.

[21] Cabinet Office Behavioural Insights Team, "Behavioural Insights Team Annual Update 2010–11," 2011.

[22] Cabinet Office Behavioural Insights Team, "Behavioural Insights Team Annual Update 2010–11," 2011, p. 17.

[23] Australian Government, "Data-Matching Program (Assistance and Tax) Act 1990," *C2006C00591*, 1990.

supposed to.[24] It seems that the promise of behavioral research-driven policy fueled by data matching techniques allows for the blending of formerly distinct roles of public authorities. The next section investigates these different governmental roles in more detail.

3.1 Two classic roles of government

In daily life, government plays a multitude of roles, which precludes a simple categorization of its roles and responsibilities. For instance, approaches towards definitions of the modern state include, with reference to Weber, Hobbes, and Marx, amongst others, the monopoly of the means of violence, sovereignty, public bureaucracy, and citizenship.[25] However, two faces can be discerned that are readily recognizable. The first one is the government's administrative face. In this role, it takes care of administrative tasks to the benefit of the citizen, such as supplying official documents like passports and driving licenses. It also exercises community functions (e.g. supplying building permits), organizes and upholds certain facilities for the benefit of the people (e.g. the educational system) and takes the lead in large projects that would be beyond the capacities of individual citizens (e.g. large infrastructural works). Although political preferences of the day dictate to what extent the government should play a role in any of these areas, all functions have in essence been delegated to the government for reasons of fairness, efficiency, and effectiveness. This is the area in which the authorities are perceived as delivering 'services' to the citizens.

The second face of government is its enforcement face. This is the area in which it upholds the law, and executes associated tasks like crime prevention and criminal prosecution. For these purposes, the government is bestowed with investigative powers that are strictly regulated and may only be exercised if certain conditions are met. Also, only specified actors within the government domain, of which the police are a prime example, may use these powers. The distinction between the administrative face and the enforcement face of government is not clear-cut in every area. Take for instance the tax domain. Many of the tasks belong to the administrative realm, such as the yearly processing of income tax filings and the collection of the amounts due. However, tax authorities are granted enforcement powers as well, which may be exercised in order to collect assets from tax subjects who are unwilling to pay, or to commence investigative actions when tax fraud is suspected.

In practice, the two faces can be distinguished in most Western jurisdictions, even though the exact definition of the purpose of the state and the scope of this purpose shows variations. This is due to differences in the development process of the state and its functions, in particular between civil law jurisdictions as can be found on the

---

[24] „Ultimately, improving data matching will help us to better measure the effectiveness of multiple programs, and more efficiently target resources to achieve goals like promoting more work and earnings, reducing poverty, and ending dependence on government benefits. These are goals that we should all agree on.", U.S. House of Representatives, Committee on Ways and Means, *Human Resources Subcommittee Hearing on the Use of Data Matching to Improve Customer Service, Program Integrity, and Taxpayer Savings*, March 11, 2011.

[25] C. Pierson, *The Modern State*. (London: Routledge, 2004), pp. 4-26.

European continent and the Common Law tradition of the United Kingdom. The UK is a state, but not a nation, and its evolvement has taken place along the lines of rather uncoordinated events that, step by step, developed the legal relations between the state and the citizens, as well as the distribution of powers.[26]

At a more fundamental level, the two faces can be related to the classical (democratic) constitutional state and the social constitutional state. In the classical constitutional state, the role of the government was mainly related to the protection of constitutional rights based on fundamental rights. In order to offer this protection, certain acts, such as murder, violence, and discrimination, were legally prohibited, and the state was empowered with enforcement capacities to uphold the law. This role of the state can also be referred to as *Ordnungspolitik* or the aggrandizement of power of the *Machtstaat*.[27] This role forms the basis of the investigative powers related to the enforcement face.[28] The social constitutional state is offering more 'social' protection, such as health care and education, and employment facilities. This is more related to the administrative face, including regulating health care standards and providing documents that allow people to work or receive education.[29] Other indications for this role are the *soziale Gestaltungspolitik* or the 'educative state' as the basis of social morality.[30]

Tensions ensue when, in the interaction with citizens, government presents its administrative face using information, which it may only have gathered in its enforcement role. The first case supplied in the previous section is a good example of this practice. ANPR data, the collection of which is sanctioned by the government's enforcement powers, are used to directly address people through channels that — until that day — have been used as the administrative face of government. The example illustrates a tendency amongst policymakers in which administrative and law enforcement tasks blend into each other. However, it should be borne in mind that administrative duties and law enforcement are based on distinct competences that through policies such as the one described above may become mingled. This raises questions of foreseeability, legitimacy and accountability of government policy. Proactive government policy may be more efficient; it can also be intrusive and premised on an authority that is legally suspect.

---

[26] J. Alder, *Constitutional and Administrative Law*. (Hampshire: Palgrave Macmillan, 2005), pp. 94-95.

[27] K.H.F. Dyson, *The State Tradition in Western Europe; A Study of an Idea and Institution*. (Oxford: Martin Robertson, 1980), p. 223.

[28] M.C. Burkens et al., *Beginselen Van De Democratische Rechtsstaat*. 5th ed. (Deventer: W.E.J. Tjeenk Willink, 2001), p. 18.

[29] M.C. Burkens et al., *Beginselen Van De Democratische Rechtsstaat*. 5th ed. (Deventer: W.E.J. Tjeenk Willink, 2001), p. 26.

[30] K.H.F. Dyson, *The State Tradition in Western Europe; A Study of an Idea and Institution*. (Oxford: Martin Robertson, 1980), p. 223.

4 Control vs. investigation

It is useful to distinguish between two typical powers that may be invoked by authorities to uphold the law, 'control' and 'investigation'.[31] Actually, these two powers have their own distinctive competences attributed to authorities. First, the power of 'control' allows the authorities to check whether the general public adheres to the rules as codified in law. One example are speed traps: by measuring the velocity of all passing vehicles at a designated spot, it is possible to probe whether the drivers adhere to the limits set out in the law. The characteristics of 'control' are twofold. First, it is not required that an unlawful act has been committed before the control mechanism is employed. By definition, it is only by using the control mechanism that unlawful acts can be detected, and control measures therefore have a preventative nature.[32] Thus, setting up a speed trap does not require the evidence that people have been speeding at that location. A second important characteristic is that control is indiscriminate (i.e. not personalized). Any subject that satisfies the definitions in the law (e.g., drivers of motor vehicles) is checked when the control mechanism is put in place, without any knowledge (nor interest, for that matter) about the identity of the driver. It is only after an offense has been established that the identity of the driver is required, because an essential element of enforcing this particular law is to fine the responsible driver for his failure to observe the set speed limits. In cases where rights and freedoms of citizens may be affected, the exercise of control measures has to be legitimized by legal provisions. Moreover, there may be no conflict with non-codified law nor with general legal principles.[33]

The second power is the power of 'investigation'. In such a case, there is always an immediate cause to start an investigation. One reason may be that it is obvious that a crime has been committed (e.g., a murder victim is found), or if there is a strong suspicion that a criminal act has occurred (e.g., the data provided on a tax return give the impression of fraudulent behavior). When the criminal investigation is started, there is often already someone suspected (e.g. the filer of the tax return), which contrasts with the concept of 'control' introduced above. Even when there is no suspect yet, for instance in a murder case without any witnesses, the investigation is still aimed at discovering the identity of the individual responsible for the crime. In other words, investigations are conducted only after sufficient justification is established in the form of substantial evidence or specific suspect behavior. Investigative powers are therefore applied in an *ex post* fashion. The use of investigative competences requires a concrete suspicion of a criminal act.[34] This act has to be punishable as provided by a specific legal provision, which implies that as

---

[31] G.J.M. Corstens, *Het Nederlands Strafprocesrecht*, 3rd ed. (Deventer: Gouda Quint, 1999), p. 21.

[32] G.P.A. Aler, *De Politiebevoegdheid Bij Opsporing En Controle* (Zwolle: W.E.J. Tjeenk Willink, 1982), p. 4 and 30.

[33] G.J.M. Corstens, *Het Nederlands Strafprocesrecht*, 3rd ed. (Deventer: Gouda Quint, 1999), p. 22.

[34] G.P.A. Aler, *De Politiebevoegdheid Bij Opsporing En Controle* (Zwolle: W.E.J. Tjeenk Willink, 1982), p. 29.

long as there is no punishable act, the exercise of investigative powers is not allowed.[35]

Tensions arise when control measures take the form of an investigation. This is the case in the first case supplied in section 2. There are rules about the conditions under which a taxpayer may claim exemption to having to pay additional taxes on the use of a company car. Ordinarily, these rules would be upheld through the process of control: after the tax return has been filed, a check would be performed on all company car drivers to see whether they adhere to the rules. Only after a suspicion arises that some of these claimants have not played by the book, an investigation may be conducted into the details of the individual tax returns of these drivers. Thus, the move from the control regime to the investigation regime (and the associated move from a general regime to an individualized regime) is only made after establishing suspicious behavior. This is, once again, an example of *ex post* investigation.

In this case, the individuals are subject to an investigative approach before they have filed their tax return, i.e. before there is any data provided by the tax subjects themselves, which might garner an interest by the investigating authorities. Instead, the data leading to an individual investigation are collected using a 'control' approach, in which first all vehicles present at a certain location and time are registered using ANPR with the specific purpose to enforce taxation laws.[36] Then, a data match is conducted, in which all company car drivers who have indicated that they are planning to stay within the 500 km exemption are highlighted. Only this specific subset is addressed in a one-to-one 'reminder' by the tax authorities. It is important to remember that the presence at that time and location in itself is not illegal, as the occasional trip to the IKEA may well fall within the limits of the 500 'private' km cap. Only if these drivers would claim on their tax returns not to have exceeded the 500 km cap and proof would show this to be a misrepresentation of facts, there would be a good case for an individual investigation. Instead of the *ex post* investigation which is customary in case of criminal investigations, the *ex ante* investigation which befalls the company car drivers concerned represents a radical new notion of the authorities' enforcement role, as will be further analyzed in the next section.

5 Analysis

In all three cases of section 2, surveillance elements are present, but the means of data collection and the presentation of data analysis findings to the individuals differ.

In the case of the ANPR "ring of steel" around the town of Royston, the data are collected on account of the enforcement powers of the authorities. In fact, the Royston case is a demonstration of a 'control' approach, which moves to investigation after a match with any of the connected databases occurs. This approach is becoming

[35] G.J.M. Corstens, *Het Nederlands Strafprocesrecht*, 3rd ed. (Deventer: Gouda Quint, 1999), p. 15.

[36] In a similar fashion, speed cameras are used as a tool to enforce speed limits and to catch speeding incidents, Both approaches qualify as control measures, because all cars within reach of the cameras are recorded *for a specific purpose that has been defined in advance*.

increasingly prevalent, and is a demonstration of the electronic execution of traditional enforcement powers. However, in cases where there is no match, the collected ANPR data remain on file with the authorities for up to two years, which calls into question the proportionality and subsidiarity of the measure: one can seriously wonder whether the demonstrated blanket surveillance and massive data collection meet these criteria. The consequence of this long-term data retention of detailed ANPR data is that the potential for an individual investigation keeps looming, and may be triggered by circumstances that are unknown at the time of registration. If such an investigation would befall any of the individuals whose vehicle is associated with any misdemeanor in the future, the authorities are likely to exercise all enforcement powers available to them.

In contrast to the above case, the example of data matching to prevent fraud in the UK does not use surveillance data recorded on account of an enforcement power. Instead, commercially available information is acquired and combined with information on file with the authorities. In principle, any output that would result in a high suspicion of benefit fraud would lend itself to the start of an investigation aimed at specific individuals, but in this case authorities decided to ask benefits recipients whether their files still reflected the actual situation. The advantages of this approach are obvious: one well-written reminder has an immediate and sizable effect, and does away with the necessity of commencing individual investigations that may take much time and effort (and funds) to complete in accordance with the strictly defined legal provisions. Thus, some of the data used are obtained from non-governmental sources, and the people who are suspect are approached individually. As opposed to the Royston case, the consequence of this strategy is that the authorities cannot use their enforcement face, since no official investigation has been started: the communication must necessarily be drafted as an administrative matter.

A similar situation exists in the case of the company car drivers, in which no crime has been committed before the drivers file a fraudulent tax return, which is why the authorities cannot rely on their enforcement face. Still, they want to stimulate taxpayers to represent the facts concerning the private use of their cars correctly, which explains why they have to revert to their administrative face and present their findings as a service to the individual company car drivers, in spite of the fact that relevant data have been gathered through enforcement competences. Surveillance as a Service sees the light, and the practice may be considered as intimidating by many company car drivers, particularly because the individualized approach normally reserved for criminal investigations is now applied in a situation which would only justify a regular ‘control’ procedure.

The last two cases are also applications of behavioral economics in policy circles, a trend that was highlighted in section 3. The mere suggestion by the authorities of their willingness to apply their enforcement powers intends to nudge individuals into desired behavior, thus rendering a personalized investigative route superfluous. The case of the company cars is in this respect all the more remarkable, since this is an example in which surveillance data gathered by the authorities employing enforcement capabilities are actively used to steer citizen’s behavior to align with governmental objectives without reverting to investigative action.

The question remains why the phenomenon described in the three case studies triggers feelings of unease amongst many people. More importantly, the

developments discussed here are symptomatic of the use of investigative powers in a growing number of areas, spurred by the possibilities offered by new technologies. This potentially has serious consequences for the organization of society, especially concerning the power balance between the citizens and the state. In an attempt to identify certain thresholds that might be crossed in such processes we will further analyze the first case study in a step-by-step fashion.

As a starting point, it should be acknowledged that the type of fraud possible with the private use of company cars can only be combated when information is collected on the actual use of the vehicle in the year previous to filing date of the tax return. So, if someone drives a company car throughout 2012, the tax return is due only by April 1, 2013. If the authorities want to call the correctness of the tax filing into question, they would logically need to have information on the actual use in 2012 at their disposal. Otherwise, they would not be able to have any proof in case of a prosecution. The use of ANPR to collect information for such purposes is thus understandable, as it is merely deployed as a technique to collect relevant data for a specific aim at a particular location for a restricted period of time. Moreover, a proper implementation of ANPR technology would allow for immediate deletion of non-relevant data, thus staying within the confines of the purpose of the data collection (i.e., control against illegitimate private use).

It is also a logical step to match the information collected through ANPR with the identity of the individual company car driver when an actual act has occurred which would justify such a data matching procedure. This is the straightforward method of producing incriminating evidence against suspected tax evaders. So far, few people would object to this practice. However, should the data still be matched when an actual justification for that step is lacking? One may argue that this is not a problem as long as this information is kept within the confines of the tax authorities. Nevertheless, the mere act of data matching creates a new category of tax subjects, namely a group of people who have driven their car privately but who have stayed within the limits of the law. It may be claimed that, exactly because the individuals remain within the limits of the law, they do not merit special attention. Without a good reason, this category should not be created to start with, as flagging is vulnerable to function creep.[37] By creating these types of unwarranted categories, certain questionable scenarios become possible. Imagine what would happen if you were to fall into this category for a few years in a row: some tax inspector might consider you to be a high profile target for a closer inspection, although you have never strayed outside the law.

The final step is that the individual company car driver is confronted with the data match before she has committed the act of falsely representing facts on a tax return. There are serious questions to be posed concerning this proactive approach, because there has never been an act[38] to merit such individual attention by the tax authorities. The fact that a probabilistic approach to some future decision is taken ("People who go to the IKEA on Sundays with their company car are likely to commit fraud in their

---

[37] See e.g., Christine Bellamy, "Alive and Well? The 'Surveillance Society' and the Coalition," *Public Policy and Administration* 26, no. 1 (2011): 149-55, and Wetenschappelijke Raad voor het Regeringsbeleid. *iOverheid* (Amsterdam: Amsterdam University Press, 2011).

[38] In Dutch: handeling

tax return."), in fact implies that the entire concept of the "presumption of innocence" is dropped. At least, you are apparently a little less innocent if you belong to a group of people who, statistically spoken, are more likely to commit fraud.[39]

Overall, one specific effect is that the innocence of people is not used as a starting point anymore. Under Dutch law, the definition[40] of a criminal offense is a fact (which can be performing or neglecting an act) that is unlawful and attributable to blame. In the cases described in this paper, the fact mentioned in the definition is lacking. Therefore, there is no rightful justification for the use of investigative powers. More and more applications of data matching are becoming a reality thanks to the increasingly more powerful possibilities afforded by modern technologies to support massive data collection against low costs. These rapid technological developments may unwittingly underexpose the requirement of a fact for the law to apply.

6 Process modification

The analysis has shown in detail what consecutive steps are taken in cases that present surveillance as a service. Even without taking a moral stance on the acceptability of the approach, one can safely assume it yields positive effects in terms of increased tax income and a lesser need to launch costly investigations. One wonders whether the same benefits might materialize using the same (types of) technology, but without the associated surveillance aspects. In our opinion, this should be feasible by adapting the data collection and matching process in line with the suggestions provided below for the company car case. The suggestions are based on basic principles of data protection as laid down in Directive 95/46/EC.[41]

In order to examine whether people truthfully represent the actual circumstances during the time period subject to taxation, it is necessary to collect information during that period. Only by confronting the claims of the tax subjects with the evidence gathered by the tax authorities throughout the fiscal year, irregularities may become apparent, which may lead to further investigations. In case of the company cars, it is therefore acceptable that ANPR data are collected of cars at potentially suspect locations, such as border crossings during holiday weekends.

---

[39] Statistical inference using data collected through surveillance may result in social sorting, discrimination and accumulated disadvantage. See e.g., Oscar H. Gandy, "Quixotics unite! Engaging the pragmatists on rational discrimination," in *Theorizing Surveillance - the panopticon and beyond*, ed. David Lyon, (Cullompton, UK: Willan Publishing, 2008), 318-336. In this particular case, the subgroup of people who visit IKEA on Sundays is also more intensively scrutinized as a result of the classification process described. The societal effects are however less prevalent, because the subgroup is less susceptible to future discrimination.

[40] In Dutch: "Voor een strafbaar feit moet sprake zijn van een feit, dat in strijd is met het recht en waarvan de bedrijver een verwijt gemaakt kan worden (dus waaraan deze schuld heeft)", J. Remmelink, *Inleiding Tot De Studie Van Het Nederlandse Strafrecht*, 14th ed. (Arnhem: Gouda Quint B.V., 1995), p. 126.

[41] Directive 95/46/EC of the European Parliament and of the Council of 24 October 1995 on the protection of individuals with regard to the processing of personal data and on the free movement of such data, OJ L 281, 23.11.1995, p. 31–50.

The choice of so-called suspect locations is critical, as it must balance the requirement of collecting enough relevant data to be used as a basis for effective fraud investigations with the need to prevent disproportionate surveillance. This would justify the focus on times and places where one would not expect business use of company cars (e.g., the IKEA parking lot on a Sunday). A potential problem is constituted by false positives caused by the systemic consequences of the data collection setup (e.g., an IKEA employee with a company car working on Sundays, who might find herself to be the subject of a closer investigation). Such effects are inevitable, but may be perceived as an acceptable downside of the control system. It is key to understand these systemic effects in advance and treat them with due caution, such as by basing all subsequent investigative steps on the presupposition that the subject is indeed a false positive. If this is done prudently, the impact on the lives of the people finding themselves in these suspect locations may be minimized.

In the proposed modified procedure the collected data — only existing of a license plate number associated with a location and a time stamp — are not processed any further, but are stored at a secure location until the moment the tax filings are received (i.e. in the year following the year in which we want to establish the potential private use of company cars). At that time, it is possible to match the number plates of the taxpayers who claim to stay below the 500 km threshold with the number plates of vehicles that have been spotted at unusual locations. Only when the same license plate is encountered in both files, there is a justified reason to start an investigation. This is the moment in which the 'hits' may be enriched with personal data of the drivers, which may subsequently be contacted as part of an investigation. All other ANPR data may be destroyed after the initial data match, as these would not benefit any further investigative purposes.

The proposed alternative process effectively protects the interests of all people who are not concerned, and it complies better with certain principles set out in the national implementations of the European Data Protection Directive.[42] For instance, if the essential step of enriching the set of license plates with personal information of the vehicle drivers is performed after the data match between the ANPR data with the tax returns, the principle of data minimization as laid down in article 6(3) of the Directive[43] is better respected. Another example is the concept of purpose specification as expressed in Art. 6(1) (a) of the Data Protection Directive, which requires that "[…] personal data must be collected for a specified, explicit and legitimate purposes and not further processed in a way incompatible with those purposes." Once again, the enrichment of the ANPR data with additional personal information after the data match would better respect this principle[44] than the current

---

[42] Directive 95/46/EC has been implemented in the national legislation of each EU member state (e.g., the Wbp in the Netherlands and the DPA in the United Kingdom).

[43] Directive 95/46/EC of the European Parliament and of the Council of 24 October 1995 on the protection of individuals with regard to the processing of personal data and on the free movement of such data, OJ L 281, 23.11.1995, p. 31–50.

[44] We refer to the Personal Data Protection Act as the legal framework against which the processing of personal data should be assessed. Considering the nature of the cases, and the involvement of actors with investigative powers, specific laws related to these actors are relevant as well. These laws contain comparable data protection principles. The point is that

practice, because the particular processing act would be specifically linked to the express purpose of combating tax evasion. In short, both processing steps should only be taken if a specific purpose is present. The first step is building a data set for future reference, and the second step is enhancement of the data set with additional personal information of individuals whose deeds actually qualify them as a suspect (i.e. after the filing of their tax return).

The net result of data protection in this alternative model is that citizens who are not suspect are not confronted with individual 'warnings', thus protecting them from undue collection and processing of data. Moreover, clear guidelines and associated communication on the enforcement practices employed would also make such systems transparent and amenable to public (legal) scrutiny. An important consequence of our proposed model is that more ANPR data need to be retained for a longer period, which may seem counter-intuitive from a data protection perspective. However, the focus is not on the storage of the data but on their eventual use. In fact, we are encouraging authorities to exercise restraint in the further processing of data through data matching.

The proposed alternative process eliminates the individualized investigation preceding the actual act of filing a tax return, and would thus remove the surveillance character of the tax authorities' behavior. However, the authorities might still be able to effectively nudge taxpayers into filing a correct tax return. By generally announcing that the information supplied by company car drivers will be the subject of intensive scrutiny in a certain year, the prospective taxpayers may be forewarned and adjust their tax filing behavior accordingly. Such a warning may even be communicated to company car drivers only, thus targeting a specific group of taxpayers. The nudging effect of addressing the entire population of company car drivers as a group at the moment of filing the tax return instead of as individuals at a moment months prior to the filing may indeed be somewhat lower. However, it has as a distinct advantage that it does not rely on the disciplining effects of surveillance as a service.

7 Conclusion

This paper employed three cases to illustrate a shift in the relationship between the government and its citizens when it comes to the use of surveillance data for law enforcement purposes. The case of the ANPR cameras surrounding the town of Royston was a demonstration of surveillance data to be used for individual investigation after a violation of the law has been established. Because of its *ex post* character, the authorities can thus use their enforcement face during prosecution. In the case of data matching using information from commercial credit rating agencies to elicit potential fraudsters, the people targeted were not prosecuted but simply asked whether the information held on them was still accurate. As individual investigations are not under discussion yet, the authorities cannot rely on enforcement measures, but

— no matter which legal regime is applicable — the suggested alternative process respects these principles better than the current practice does.

have to present their actions as administrative matters. In the last case of the company car drivers there is again no individual prosecution, but this time the authorities rely on surveillance data obtained through enforcement powers as a basis for addressing certain citizens. This particular construct was dubbed “Surveillance as a service”, because the authorities themselves frame their actions as proactively providing services aimed at making life easier for citizens by helping them to prevent any unfortunate mistakes.

All cases use data matching as a starting point, but only the first aims to use the newly created information to start individual investigations after a violation of the law has been established. The last two cases demonstrate how the authorities aim to guide citizens into desired behavior *before* any proof of a criminal offense exists. Merely raising the awareness of the potential availability of incriminating information should be sufficient to reach certain government objectives, nudging citizens to do the right thing without having to resort to costly individual investigations.

The use of surveillance data to influence people before any factual proof exists may be considered by some as intrusive, as it removes essential elements of the expected safeguards against government interference with citizens’ private lives. By outlining a modified process with regard to the last case, we demonstrated that similar policy objectives may be attained without resorting to the potentially intimidating use of enforcement data. Although the nudging effect may be somewhat lower, the transgressive use of surveillance data to exert influence on an individualized level without proof of an unlawful act is thus constrained.

Acknowledgement The authors greatly acknowledge the anonymous reviewers for their valuable comments on draft versions of this paper.

Bibliography

Alder, J. *Constitutional and Administrative Law*. Hampshire: Palgrave Macmillan, 2005.

Aler, G.P.A. *De Politiebevoegdheid Bij Opsporing En Controle*. Zwolle: W.E.J. Tjeenk Willink, 1982.

Alfen, Sameer van. "Fiscus Bespioneert Leaserijders." *De Telegraaf*, February 11, 2011.

Australian Government. "Data-Matching Program (Assistance and Tax) Act 1990." In *C2006C00591*, 1990.

Batey, Angus. "Welcome to Royston … You're under Surveillance." *Guardian*, June 29, 2011.

Bellamy, Christine. "Alive and Well? The 'Surveillance Society' and the Coalition." *Public Policy and Administration* 26, no. 1 (2011): 149-55.

Burkens, M.C., H.R.B.M. Kummeling, B.P. Vermeulen, and R.J.G.M. Widdershoven. *Beginselen Van De Democratische Rechtsstaat*. 5th ed. Deventer: W.E.J. Tjeenk Willink, 2001.

Cabinet Office Behavioural Insights Team. "Behavioural Insights Team Annual Update 2010–11." 2011.

Corstens, G.J.M. *Het Nederlands Strafprocesrecht*. 3rd ed. Deventer: Gouda Quint, 1999.

Dyson, K.H.F. *The State Tradition in Western Europe; A Study of an Idea and Institution*. Oxford: Martin Robertson, 1980.

European Commission. "Directive 95/46/EC of the European Parliament and of the Council of 24 October 1995 on the protection of individuals with regard to the processing of

personal data and on the free movement of such data," OJ L 281, 23.11.1995, p. 31–50.

Farrier, Charles, Simon Davies, and Daniel Hamilton. "Complaint Letter to the Information Commissioner Concerning Royston Anpr “Ring of Steel”." June 7, 2011.

Hutton, Alice. "Hidden Cameras on All Routes In." *Royston Weekly News*, March 25, 2011.

"Income Taxation Act 1964 (Wet Op De Loonbelasting 1964)." 1964.

Information and Privacy Commissioner/Ontario. "Privacy Investigation: The Toronto Police Service's Use of Mobile Licence Plate Recognition Technology to Find Stolen Vehicles." 2003.

Jolls, Christine, Cass R. Sunstein, and Richard H. Thaler. "A Behavioral Approach to Law and Economics." *Stanford Law Review* 50 (1997): 1471-1550.

Kooreman, Peter, and Henriëtte Prast. "What Does Behavioral Economics Mean for Policy? Challenges to Savings and Health Policies in the Netherlands." *De Economist* 158, no. 2 (2010): 101-122.

Loewenstein, George. "Experimental Economics from the Vantage-Point of Behavioural Economics." *The Economic Journal* 109, no. February (1999): F25-F34.

Los, Maria. "Looking into the Future: Surveillance, Globalization and the Totalitarian Potential." In *Theorizing Surveillance - the Panopticon and Beyond*, edited by David Lyon, 69-94. Cullompton, UK: Willan Publishing, 2008.

Lyon, David. *Surveillance Studies: An Overview*. Cambridge: Polity Press, 2007.

Mathieson, S.A. "Privacy Groups Take Royston's ANPR Plans to ICO." *Guardian*, June 10, 2011.

O'Donnell, Gus. "Applying Behavioural Insights." Cabinet Office, http://www.cabinetoffice.gov.uk/content/applying-behavioural-insights.

Pierson, C. *The Modern State*. London: Routledge, 2004.

Remmelink, J. *Inleiding Tot De Studie Van Het Nederlandse Strafrecht*. 14th ed. Arnhem: Gouda Quint B.V., 1995.

Sluijs, Jasper. "The Dutch Tax Authority and Lease Car Fraud: Institutionalized Intimidation." http://vortex.uvt.nl/TILTblog/?p=291.

Thaler, Richard H., and Cass R. Sunstein. "Libertarian Paternalism." *The American Economic Review* 93 (2003): 175-79.

———. *Nudge: Improving Decisions About Health, Wealth, and Happiness*. 1st ed: Yale University Press, 2008.

U.S. House of Representatives, Committee on Ways and Means. "Human Resources Subcommittee Hearing on the Use of Data Matching to Improve Customer Service, Program Integrity, and Taxpayer Savings." March 11, 2011.

Wetenschappelijke Raad voor het Regeringsbeleid. *iOverheid*. Amsterdam: Amsterdam University Press, 2011.

Wintour, David. "David Cameron's 'Nudge Unit' Aims to Improve Economic Behaviour." *Guardian*, September 9, 2010.